The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- airport_express	Unspecified vulnerability in the network bridge functionality on the Apple Time Capsule, AirPort Extreme Base Station, and AirPort Express Base Station with firmware before 7.5.2 allows remote attackers to cause a denial of service (networking outage) via a crafted DHCP reply.	2010-12-21	7.1
ecava -- integraxor	Stack-based buffer overflow in the save method in the IntegraXor.Project ActiveX control in igcomm.dll in Ecava IntegraXor Human-Machine Interface (HMI) before 3.5.3900.10 allows remote attackers to execute arbitrary code via a long string in the second argument.	2010-12-23	10.0
eucalyptus -- eucalyptus	The password reset feature in the administrator interface for Eucalyptus 2.0.0 and 2.0.1 does not perform authentication, which allows remote attackers to gain privileges by sending password reset requests for other users.	2010-12-22	7.5
google -- chrome	The Pickle::Pickle function in base/pickle.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 on 64-bit Linux platforms does not properly perform pointer arithmetic, which allows remote attackers to bypass message deserialization validation, and cause a denial of service or	2010-12-21	7.5

Back to top

High Vulnerabilities			
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**
	possibly have unspecified other impact, via invalid pickle data.		
google -- chrome	Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly perform cursor handling, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."	2010-12-21	10.0
hp -- storageworks_modular_smart_array_p2000_g3_firmware	HP StorageWorks Modular Smart Array P2000 G3 firmware TS100R011, TS100R025, TS100P002, TS200R005, TS201R014, and TS201R015 installs an undocumented admin account with a default "!admin" password, which allows remote attackers to gain privileges.	2010-12-17	9.0
hp -- storageworks_storage_mirroring	Unspecified vulnerability in HP StorageWorks Storage Mirroring 5.x before 5.2.2.1771.2 allows remote attackers to execute arbitrary code via unknown vectors.	2010-12-21	10.0
hp -- power_manager	Unspecified vulnerability in HP Power Manager (HPPM) before 4.3.2 allows remote attackers to execute arbitrary code via unknown vectors.	2010-12-22	9.3
invensys -- foxboro_i/a_series_batch	Buffer overflow in the lm_tcp service in Invensys Wonderware InBatch 8.1 and 9.0, as used in Invensys Foxboro I/A Series Batch 8.1 and possibly other products, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted request to port 9001.	2010-12-17	10.0
microsoft -- windows	Unspecified vulnerability in Microsoft Windows has unknown impact and attack vectors, as reported by Moti and Xu Hao.	2010-12-22	10.0
microsoft -- ie	Use-after-free vulnerability in the CSharedStyleSheet::Notify function in the Cascading Style Sheets (CSS) parser in mshtml.dll, as used in Microsoft Internet Explorer 7 and 8 and possibly other products, allows remote attackers to cause a denial of service (crash) and execute arbitrary code via multiple @import calls in a crafted document.	2010-12-22	9.3

Back to top

High Vulnerabilities			
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**
microsoft -- iis	The TELNET_STREAM_CONTEXT::OnSendData function in the FTP protocol handler (ftpsvc.dll) for Microsoft Internet Information Services (IIS) 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted FTP request that triggers memory corruption. NOTE: some of these details are obtained from third party information.	2010-12-23	10.0
microsoft -- wmi_administrative_tools	The WBEMSingleView.ocx ActiveX control 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier allows remote attackers to execute arbitrary code via a crafted argument to the AddContextRef method, possibly an untrusted pointer dereference.	2010-12-23	9.3
microsoft -- wmi_administrative_tools	The WBEMSingleView.ocx ActiveX control 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier allows remote attackers to execute arbitrary code via a crafted argument to the ReleaseContext method, a different vector than CVE-2010-3973, possibly an untrusted pointer dereference.	2010-12-23	9.3
opera -- opera_browser	Unspecified vulnerability in Opera before 11.00 has unknown impact and attack vectors, related to "a high severity issue."	2010-12-21	10.0
opera -- opera_browser	The default configuration of Opera before 11.00 enables WebSockets functionality, which has unspecified impact and remote attack vectors, possibly a related issue to CVE-2010-4508.	2010-12-21	10.0
opera -- opera_browser	Opera before 11.00 on Windows does not properly implement the Insecure Third Party Module warning message, which might make it easier for user-assisted remote attackers to have an unspecified impact via a crafted module.	2010-12-21	9.3
pangramsoft -- pointter_php_content_management_system	Pointter PHP Content Management System 1.0 allows remote attackers to bypass authentication and obtain administrative privileges via arbitrary values of the auser and apass cookies.	2010-12-21	7.5
pangramsoft -- pointter_php_micro-blogging_social_network	Pointter PHP Micro-Blogging Social Network 1.8 allows remote attackers to bypass authentication and obtain administrative privileges via arbitrary values of the auser and apass cookies.	2010-12-21	7.5

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score
phpmyfaq -- phpmyfaq	phpMyFAQ 2.6.11 and 2.6.12, as distributed between December 4th and December 15th 2010, contains an externally introduced modification (Trojan Horse) in the getTopTen method in inc/Faq.php, which allows remote attackers to execute arbitrary PHP code.	2010-12-17	7.5
sap -- netweaver_business_client	Stack-based buffer overflow in the SapThemeRepository ActiveX control (sapwdpcd.dll) in SAP NetWeaver Business Client allows remote attackers to execute arbitrary code via the (1) Load and (2) LoadTheme methods.	2010-12-17	9.3
sap -- crystal_reports	Heap-based buffer overflow in the CrystalReports12.CrystalPrintControl.1 ActiveX control in PrintControl.dll 12.3.2.753 in SAP Crystal Reports 2008 SP3 Fix Pack 3.2 allows remote attackers to execute arbitrary code via a long ServerResourceVersion property value.	2010-12-21	9.3
symantec -- endpoint_protection	fw_charts.php in the reporting module in the Manager (aka SEPM) component in Symantec Endpoint Protection (SEP) 11.x before 11 RU6 MP2 allows remote attackers to bypass intended restrictions on report generation, overwrite arbitrary PHP scripts, and execute arbitrary code via a crafted request.	2010-12-21	7.5
tibco -- activematrix_bpm	Unspecified vulnerability in the ActiveMatrix Runtime component in TIBCO ActiveMatrix Service Grid 3.0.0, 3.0.1, and 3.1.0; ActiveMatrix Service Bus 3.0.0 and 3.0.1; ActiveMatrix BusinessWorks Service Engine 5.9.0; ActiveMatrix BPM 1.0.1 and 1.0.2; Silver BPM Service 1.0.1; and Silver CAP Service 1.0.0 allows remote authenticated users to execute arbitrary code via vectors related to JMX connections.	2010-12-17	9.0
tor -- tor	Heap-based buffer overflow in Tor before 0.2.1.28 and 0.2.2.x before 0.2.2.20-alpha allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via unspecified vectors.	2010-12-21	10.0

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score
vmware -- esxi	The Update Installer in VMware ESXi 4.1, when a modified sfcb.cfg is present, does not properly configure the SFCB authentication mode, which allows remote attackers to obtain access via an arbitrary username and password.	2010-12-22	9.3

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- airport_express	The ICMPv6 implementation on the Apple Time Capsule, AirPort Extreme Base Station, and AirPort Express Base Station with firmware before 7.5.2 does not limit the rate of (1) Router Advertisement and (2) Neighbor Discovery packets, which allows remote attackers to cause a denial of service (resource consumption and device restart) by sending many packets.	2010-12-21	6.1	CVE-2009-2189 CONFIRM APPLE
collectd -- collectd	The cu_rrd_create_file function (src/utils_rrdcreate.c) in collectd 4.x before 4.9.4 and before 4.10.2 allow remote attackers to cause a denial of service (assertion failure) via a packet with a timestamp whose value is 10 or less, as demonstrated by creating RRD files using the (1) RRDtool and (2) RRDCacheD plugins.	2010-12-17	5.0	CVE-2010-4336 VUPEN BID DEBIAN SECUNIA SECUNIA CONFIRM CONFIRM
earl_miles -- views	Multiple cross-site request forgery (CSRF) vulnerabilities in the Views UI implementation in the Views module 5.x before 5.x-1.8 and 6.x before 6.x-2.11 for Drupal allow remote attackers to hijack the authentication of administrators for requests that (1) enable all Views or (2) disable all Views.	2010-12-23	6.8	CVE-2010-4519 MLIST MLIST CONFIRM
earl_miles -- views	Multiple cross-site scripting (XSS) vulnerabilities in the Views module 6.x before 6.x-2.11 for Drupal allow remote attackers to inject arbitrary web script or HTML via (1) a URL or (2) an aggregator feed title.	2010-12-23	4.3	CVE-2010-4520 MLIST MLIST CONFIRM
earl_miles -- views	Cross-site scripting (XSS) vulnerability in the Views module 6.x before 6.x-2.12 for Drupal allows remote attackers to inject arbitrary web script or HTML via a page path.	2010-12-23	4.3	CVE-2010-4521 MLIST MLIST CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
ecava -- integraxor	Directory traversal vulnerability in Ecava IntegraXor 3.6.4000.0 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the file_name parameter in an open request.	2010-12-23	5.0	CVE-2010-4598 VUPEN BID EXPLOIT-DB MISC
ecava -- integraxor	Untrusted search path vulnerability in Ecava IntegraXor 3.6.4000.0 allows local users to gain privileges via a Trojan horse dwmapi.dll file in the current working directory. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2010-12-23	6.9	CVE-2010-4599 BID
git -- git	Cross-site scripting (XSS) vulnerability in Gitweb 1.7.3.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) f and (2) fp parameters.	2010-12-17	4.3	CVE-2010-3906 BID MANDRIVA EXPLOIT-DB SECUNIA
google -- chrome	The ThemeInstalledInfoBarDelegate::Observe function in browser/extensions /theme_installed_infobar_delegate.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle incorrect tab interaction by an extension, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted extension.	2010-12-21	4.3	CVE-2010-4575 CONFIRM CONFIRM CONFIRM
google -- chrome	browser/worker_host /message_port_dispatcher.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle certain postMessage calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code that creates a web worker.	2010-12-21	5.0	CVE-2010-4576 CONFIRM CONFIRM CONFIRM
google -- chrome	Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.	2010-12-21	5.0	CVE-2010-4577 CONFIRM CONFIRM
hp -- openvms	Unspecified vulnerability in HP OpenVMS 8.3, 8.3-1H1, and 8.4 on the Itanium platform on Integrity servers allows local users to gain privileges or cause a denial of service via unknown	2010-12-22	5.7	CVE-2010-4110 VUPEN BID SECUNIA HP

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vectors.			HP
hp -- insight_diagnostics	Cross-site scripting (XSS) vulnerability in HP Insight Diagnostics Online Edition before 8.5.1.3712 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-12-22	4.3	CVE-2010-4111 HP HP
hp -- insight_management_agents	HP Insight Management Agents before 8.6 allows remote attackers to obtain sensitive information via an unspecified request that triggers disclosure of the full path.	2010-12-22	5.0	CVE-2010-4112 VUPEN BID SECUNIA HP HP
hp -- discovery&dependency_mapping_inventory	Cross-site scripting (XSS) vulnerability in HP Discovery & Dependency Mapping Inventory (DDMI) 2.5x, 7.5x, and 7.6x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-12-22	4.3	CVE-2010-4114 HP HP
ibm -- websphere_service_registry_and_repository	IBM WebSphere Service Registry and Repository (WSRR) 7.0.0 before FP1 does not properly implement access control, which allows remote attackers to perform governance actions via unspecified API requests to an EJB interface.	2010-12-22	5.0	CVE-2010-2644 XF CONFIRM AIXAPAR
ibm -- enovia	Cross-site scripting (XSS) vulnerability in IBM ENOVIA 6 allows remote attackers to inject arbitrary web script or HTML via vectors related to the emxFramework.FilterParameterPattern property.	2010-12-22	4.3	CVE-2010-4589 VUPEN BID AIXAPAR CONFIRM
ibm -- lotus_mobile_connect	Cross-site scripting (XSS) vulnerability in HTTP Access Services (HTTP-AS) in the Connection Manager in IBM Lotus Mobile Connect (LMC) before 6.1.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-12-22	4.3	CVE-2010-4590 VUPEN CONFIRM AIXAPAR SECTRACK
ibm -- lotus_mobile_connect	The Connection Manager in IBM Lotus Mobile Connect (LMC) before 6.1.4, when HTTP Access Services (HTTP-AS) is enabled, does not delete LTPA tokens in response to use of the iNotes Logoff button, which might allow physically proximate attackers to obtain access via an unattended client, related to a cookie domain mismatch.	2010-12-22	4.4	CVE-2010-4591 CONFIRM AIXAPAR
ibm -- lotus_mobile_connect	The Mobile Network Connections functionality in the Connection Manager in IBM Lotus Mobile Connect before	2010-12-22	4.3	CVE-2010-4592 CONFIRM AIXAPAR

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	6.1.4, when HTTP Access Services (HTTP-AS) is enabled, does not properly handle failed attempts at establishing HTTP-TCP sessions, which allows remote attackers to cause a denial of service (memory consumption and daemon crash) by making many TCP connection attempts.			
ibm -- lotus_mobile_connect	The Connection Manager in IBM Lotus Mobile Connect before 6.1.4 does not properly maintain a certain reference count, which allows remote authenticated users to cause a denial of service (IP address exhaustion) by making invalid attempts to establish sessions with the same VPN ID from multiple devices.	2010-12-22	4.0	CVE-2010-4593 CONFIRM AIXAPAR
ibm -- lotus_mobile_connect	The Connection Manager in IBM Lotus Mobile Connect before 6.1.4, when HTTP Access Services (HTTP-AS) is enabled, does not properly process TCP connection requests, which allows remote attackers to cause a denial of service (memory consumption and HTTP-AS hang) by making many connection requests that trigger "queue size delta errors," related to a "timing hole" issue.	2010-12-22	4.3	CVE-2010-4594 CONFIRM AIXAPAR
ibm -- lotus_mobile_connect	The Connection Manager in IBM Lotus Mobile Connect before 6.1.4 disables the http.device.stanza blacklisting functionality for HTTP Access Services (HTTP-AS), which allows remote attackers to bypass intended access restrictions via an HTTP request that contains a disallowed User-Agent header.	2010-12-22	5.0	CVE-2010-4595 CONFIRM AIXAPAR
intel -- intel_alert_management_system	The GetStringAMSHandler function in prgxhndl.dll in hndlrsvc.exe in the Intel Alert Handler service (aka Symantec Intel Handler service) in Intel Alert Management System (AMS), as used in Symantec Antivirus Corporate Edition 10.1.4.4010 on Windows 2000 SP4 and Symantec Endpoint Protection before 11.x, does not properly validate the CommandLine field of an AMS request, which allows remote attackers to cause a denial of service (application crash) via a crafted request.	2010-12-22	5.0	CVE-2010-3268 XF VUPEN BUGTRAQ MISC SECUNIA
isc -- dhcp	ISC DHCP server 4.2 before 4.2.0-P2, when configured to use failover partnerships, allows remote attackers to	2010-12-17	5.0	CVE-2010-3616 CERT-VN CONFIRM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cause a denial of service (communications-interrupted state and DHCP client service loss) by connecting to a port that is only intended for a failover peer, as demonstrated by a Nagios check_tcp process check to TCP port 520.			MLIST VUPEN SECTRACK SECUNIA
jovelstefan -- embedded-video	Cross-site scripting (XSS) vulnerability in lembedded-video.php in the Embedded Video plugin 4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the content parameter to wp-admin/post.php.	2010-12-22	4.3	CVE-2010-4277 XF BID BUGTRAQ
linux -- kernel	The ACPI subsystem in the Linux kernel before 2.6.36.2 uses 0222 permissions for the debugfs custom_method file, which allows local users to gain privileges by placing a custom ACPI method in the ACPI interpreter tables, related to the acpi_debugfs_init function in drivers/acpi/debugfs.c.	2010-12-22	6.9	CVE-2010-4347 CONFIRM MLIST MLIST CONFIRM XF BID CONFIRM EXPLOIT-DB
opera -- opera_browser	Opera before 11.00 does not properly constrain dialogs to appear on top of rendered documents, which makes it easier for remote attackers to trick users into interacting with a crafted web site that spoofs the (1) security information dialog or (2) download dialog.	2010-12-21	5.0	CVE-2010-4579 CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 11.00 does not clear WAP WML form fields after manual navigation to a new web site, which allows remote attackers to obtain sensitive information via an input field that has the same name as an input field on a previously visited web site.	2010-12-21	5.0	CVE-2010-4580 CONFIRM CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 11.00 does not properly handle security policies during updates to extensions, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.	2010-12-21	5.0	CVE-2010-4582 CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Unspecified vulnerability in the auto-update functionality in Opera before 11.00 allows remote attackers to cause a denial of service (application crash) by triggering an Opera Unite update.	2010-12-21	5.0	CVE-2010-4585 CONFIRM CONFIRM CONFIRM
phpmyadmin -- phpmyadmin	phpMyAdmin before 3.4.0-beta1 allows remote attackers to bypass authentication and obtain sensitive information via a direct request to phpinfo.php, which calls	2010-12-17	5.0	CVE-2010-4481 CONFIRM CONFIRM VUPEN

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the phpinfo function.			SECUNIA
rim -- blackberry_enterprise_server	Multiple buffer overflows in the PDF distiller component in the BlackBerry Attachment Service in BlackBerry Enterprise Server 5.0.0 through 5.0.2, 4.1.6, and 4.1.7 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PDF document.	2010-12-17	6.8	CVE-2010-2602 XF VUPEN SECTRACK BID CONFIRM SECUNIA
xfig -- xfig	Stack-based buffer overflow in Xfig 3.2.4 and 3.2.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a FIG image with a crafted color definition.	2010-12-17	6.8	CVE-2010-4262 CONFIRM FEDORA MISC VUPEN BID MLIST MLIST SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- airport_express	The Application-Level Gateway (ALG) on the Apple Time Capsule, AirPort Extreme Base Station, and AirPort Express Base Station with firmware before 7.5.2 modifies PORT commands in incoming FTP traffic, which allows remote attackers to use the device's IP address for arbitrary intranet TCP traffic by leveraging write access to an intranet FTP server.	2010-12-21	2.6	CVE-2010-0039 CONFIRM APPLE
dmasoftlab -- radius_manager	Multiple cross-site scripting (XSS) vulnerabilities in Radius Manager 3.8.0 allow remote authenticated administrators to inject arbitrary web script or HTML via the (1) name or (2) descr parameter in an (a) update_usergroup or a (b) store_nas action to admin.php.	2010-12-21	3.5	CVE-2010-4275 XF BID EXPLOIT-DB SECUNIA
linux -- kernel	The install_special_mapping function in mm/mmap.c in the Linux kernel before 2.6.37-rc6 does not make an expected security_file_mmap function call, which allows local users to bypass intended mmap_min_addr restrictions and possibly conduct NULL pointer dereference attacks via a crafted assembly-language application.	2010-12-22	2.1	CVE-2010-4346 CONFIRM MLIST MLIST MLIST MLIST CONFIRM MLIST CONFIRM SECUNIA
linux -- kernel	arch/x86/kvm/x86.c in the Linux kernel before 2.6.36.2 does not initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory via read operations on the /dev/kvm device.	2010-12-23	1.9	CVE-2010-3881 CONFIRM MLIST BID MLIST

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST CONFIRM CONFIRM VUPEN CONFIRM SECTRACK REDHAT
opera -- opera_browser	Opera before 11.00, when Opera Turbo is enabled, does not display a page's security indication, which makes it easier for remote attackers to spoof trusted content via a crafted web site.	2010-12-21	2.6	CVE-2010-4583 CONFIRM CONFIRM CONFIRM
opera -- opera_browser	Opera before 11.00, when Opera Turbo is used, does not properly present information about problematic X.509 certificates on https web sites, which might make it easier for remote attackers to spoof trusted content via a crafted web site.	2010-12-21	2.6	CVE-2010-4584 CONFIRM CONFIRM CONFIRM
rim -- blackberry_desktop_software	RIM BlackBerry Desktop Software 4.7 through 6.0 for PC, and 1.0 for Mac, uses a weak password to encrypt a database backup file, which makes it easier for local users to decrypt the file via a brute force attack.	2010-12-17	2.1	CVE-2010-2603 BID CONFIRM SECUNIA SECUNIA

Back to top